Правила игры в 21[1]

С выходом 21 приказа ФСТЭК России в области ИБ остались актуальными два извечных вопроса: «Что делать?» и «Кто виноват?» Рассмотрим первый из них, в части 21 приказа ФСТЭК России.

***Владимир Журавлев**, преподаватель, эксперт, ответственный за организацию обработки ПДн в учебном центре «Информзащита»*

Существует несколько точек зрения на применение 21 приказа ФСТЭК России при определении мер по защите ПДн.

Вариант № 1. Часть экспертов признали его достаточным для выполнения требований по защите ПДн. Остальные же документы: Постановление Правительства № 1119 и ФЗ № 152 «О персональных данных», а также Конституция России остаются как бы в стороне, так как являются документами слишком высокого уровня.

Пользоваться только «долгожданным» приказом при определении мер по обеспечению безопасности ИБ можно, но не всегда эффективно. Рассмотрим пример.

Предложенная в 21 приказе модель выбора мер по обеспечению безопасности ПДн (п. 9) выглядит следующим образом.

Шаг № 1. *Определение* базового набора мер по обеспечению безопасности ПДн для установленного уровня защищенности (УЗ) ПДн.

Шаг № 2. *Адаптация* базового набора… с учетом:

- структурно-функциональных характеристик информационной системы;
- информационных технологий;
- особенностей функционирования информационной системы (*в том числе исключение* из базового набора мер, непосредственно связанных с информационными технологиями…).

Шаг № 3. *Уточнение* адаптированного базового набора мер… *с учетом не выбранных ранее мер*, …в результате чего определяются меры, направленные на нейтрализацию всех актуальных угроз безопасности.

Шаг № 4. *Дополнение* уточненного адаптированного базового набора мер… *установленными иными нормативными правовыми актами* в области обеспечения безопасности ПДн и *защиты информации.*

Если строить систему защиты, опираясь *только* на п. 9, то на перечень мер по обеспечению безопасности окажут влияние три фактора:

1) уровень защищенности (определяющий шаг № 1);

2) структура ИСПДн и используемые технологии (шаг № 2), пример: нет виртуализации – нет и требований по ее защите;

3) дополнительные обязательные требования, закрепленные в иных ФЗ и нормативных актах (шаг № 4).

Шаг № 3 хотя и является ключевым (о чем будет рассказано далее), будет пропущен, так как непонятно, как и, главное, зачем оператору уточнять «адаптированный набор базовых мер» с учетом НЕ выбранных мер (то есть принимать дополнительные меры).

Кроме этого, при таком подходе непонятно, какие конкретно требования предъявляются к СЗИ для обеспечения безопасности ПДн. Пример: требование СОВ. 1 (система обнаружения вторжений) предусматривает… (играет напряженная музыка) «обнаружение вторжений». Все! Вопросы: Как? Какие? Когда? и т. д. остаются «за кадром» 21 приказа, лишь в п. 12 идет привязка уровня защищенности ИСПДн к классу СОВ, установленному ФСТЭК России при использовании «сертифицированных средств защиты»[2]. Перед оператором будет стоять вопросы: «Какую из них выбрать?», и «Почему не самую дешевую из представленных на рынке?», и «Нужна ли мне „сертифицированная СОВ“? Именно 21 приказ на указанные вопросы не отвечает.

Однако в таком подходе есть и приятная сторона. Если вам (оператору) лень разбираться в построении модели угроз, актуализации и т. д., 21 приказ позволяет с учетом

[1] *Изучая 21 приказ ФСТЭК России, складывается устойчивое впечатление, что за основу были взяты «западные стандарты» и сделана попытка адаптации их под российское законодательство. Согласно Википедии, игра в 21 очко «…была изобретена в СССР как вариант игры блэкджек, в который возможно играть стандартной русской колодой (36 карт) вместо полной стандартной колоды (52 карты)»*

[2] *Данный пункт также создает предпосылки для споров. В самом 21 приказе используется разная терминология в отношении средств защиты. Определения «прошедших процедуру оценки соответствия» в п. 4 и «сертифицированных» в п. 12 сильно отличаются лексически, а возможно, и по смыслу, вложенному в них ФСТЭК России.*

уровня защищенности получить перечень требований и установить соответствующие СЗИ с мотивировкой «потому что!» Такой подход существенно снижает затраты на разработку документов (модель угроз становится формальным документом)[3], но может значительно увеличить затраты на СЗИ. Кроме этого, он мало учитывает здравый смысл (СЗИ в таком случае защищают от закона, а не от злоумышленников) и усложняет обоснование отсутствия «экономической целесообразности» для отказа от использования части рекомендованных мер защиты[4].

Вариант № 2. Данный вариант основан на «актуализации угроз». Так, в Постановлении Правительства № 1119 п. 2, а также в 21 приказе ФСТЭК России присутствует важное требование: «*Безопасность ПДн* при их обработке в информационной системе *обеспечивается с помощью системы защиты персональных данных, **нейтрализующей актуальные угрозы***, определенные в соответствии с частью 5 статьи 19 Федерального закона „О персональных данных“.

Система защиты ПДн включает в себя организационные и (или) технические ***меры, определенные с учетом актуальных*** угроз безопасности ПДн…».

В переводе с юридического на русский это значит, что ключевым элементом является определение актуальности угроз, именно актуальные угрозы надо нейтрализовать с «применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации»[5].

При определении актуальных угроз нам могут помочь два «старых», но не отмененных документа: «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн», а также «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», утвержденные ФСТЭК России 15 февраля 2008 года. Забавно, что «Базовая модель…» разрабатывалась во исполнение 781 Постановления Правительства, но не имеет ссылки на указанный документ, а также фактически не привязана к классам ИСПДн. «Методика определения актуальных угроз…» лишь символически ссылается на 781 Постановление Правительства и в последнем абзаце закрепляет то, что формирование конкретных требований необходимо производить «с использованием ***данных о классе*** ИСПДн». Таким образом, при переходе от «Классов» к «Уровням защищенности» в применении указанных документов ничего не поменялось.

Следующий важный вопрос: а что нам дает модель угроз и актуализация? Ответ прост: именно эти документы позволяют формально обосновать минимизацию используемых «средств защиты»[6] и, как следствие, затрат на их приобретение.

Последовательность действий можно представить в следующем виде.

0. Назначение ответственного и сбор необходимой информации об ИСПДн (без этого провести дальнейшие работы невозможно).

1. Акт «классификации» ИСПДн. Цель – определение «уровня защищенности».

2. Построение модели угроз. Цель – определение перечня актуальных угроз[7].

3. Определение базового набора мер (это шаг № 1)[8]. Зная УЗ ИСПДн, можно определиться с объемом и составом рекомендуемых мер по обеспечению безопасности согласно 21 приказу. Объем «бедствия» – мер по защите – следующий: УЗ-4 – 27 мер, УЗ-3 – 41 мера, УЗ-2 – 64 меры, УЗ-1 – 69 мер).

4. Адаптация (шаг № 2). Зная, как построена наша ИСПДн, мы можем исключить часть мер по защите ПДн, направленных на нейтрализацию угроз, которые у вас отсутствуют. Например, у вас нет виртуализации, значит, рекомендации по разделу «XI. Защита среды виртуализации (ЗСВ)» можно даже не открывать.

5. Уточнение ч. 1 (шаг № 3). После адаптации набор мер может остаться значительным. Для его дальнейшего сокращения понадобится «Модель угроз», а также ссылка на нейтрализацию «актуальных угроз»[9], которая позволяет заявлять, что если угроза признана неактуальной, то для ее нейтрализации не требуется использовать средства защиты, а достаточно уже принятых мер. Например, у вас установлена не сертифицированная/не прошедшая процедуру оценки соответствия система обнаружения вторжений, НО такие угрозы, как удаленный запуск приложений[10] или внедрение ложного объекта сети[11] и иные, которые можно нейтрализовать с помощью СОВ, признаны неактуальными. Следовательно, устанавливать сертифицированную/прошедшую оценку соответствия СОВ вам не требуется. (Самое главное, что это можно документально обосновать, со ссылкой на методические документы ФСТЭК России.) Это может быть важным в свете п. 12 приказа № 21 ФСТЭК России, где жестко закреплена привязка классов сертифицированных средств защиты к УЗ.

---

[3] *Предусмотрена ФЗ № 152 «О персональных данных» ст. 19 ч. 2 п. 1 «определением угроз безопасности…».*

[4] *Предусмотрено в п. 10 приказа № 21 ФСТЭК России.*

[5] *Постановление Правительства № 1119 ч. 13 п. «г»: «использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз».*

[6] *«…применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации».*

[7] *При правильном описании ИСПДн и разбиении ее на части некоторые угрозы можно признать НЕактуальными. Рассмотрение построения модели угроз с последующей актуализацией достойно отдельной статьи.*

[8] *П. 9 Приказа № 21 ФСТЭК России.*

[9] *Постановление Правительства № 1119, п. 2 и Приказ № 21 ФСТЭК России, п. 3.*

[10] *П. 6.2. Базовая модель угроз (для АРМ, имеющего подключения к сетям общего пользования).*

[11] *П. 6.5 или 6.6. Базовая модель угроз (для распределенных ИСПДн).*

6. Уточнение ч. 2. (по-прежнему шаг № 3). Зная набор актуальных угроз, можно:

- подобрать соответствующее средство защиты с минимально необходимым набором функций;
- заменить рекомендуемую меру по защите на компенсирующую (из рекомендованных в 21 приказе), если у вас уже стоит СЗИ с соответствующим функционалом;
- разработать свою меру, направленную на нейтрализацию актуальной угрозы (с обоснованием применения такой меры)[12].

7. Уточнение ч. 3 (все еще шаг № 3). В случае если угроза признана актуальной, но для ее нейтрализации не предусмотрено обязательных мер, для данного УЗ (например, защиты от утечки по техническим каналам (ЗТС. 1)) можно пойти тремя путями:

- выполнить «компенсационную меру» ЗТС. 1 (с учетом НЕ выбранных мер);
- разработать «свою» меру по нейтрализации угрозы;
- выполнить все обязательные меры, но не более того, то есть ничего не делать и не защищаться от данной угрозы.

8. Уточнение ч. 4 (Да! Это все еще шаг № 3). Данный пункт приобретет актуальность, если вы используете «новые» технологии или выявили новую угрозу (что также теоретически возможно), для которых не определены меры по обеспечению безопасности. В данном случае следует поступать аналогично с предыдущим пунктом.

9. Дополнение (шаг № 4). Если законодательством на вас возложены дополнительные обязанности по защите информации, то придется реализовывать и дополнительные меры. Кроме этого, следует помнить, что требования, указанные в Постановлении Правительства № 1119, необходимо выполнить и их нельзя актуализировать. Например, для УЗ-1 необходимо «создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности». Значит, ответственное структурное подразделение должно быть назначено или создано. В него теоретически может входить даже один сотрудник, хотя это будет лишь формальным выполнением требований.

Вместо заключения хочется отметить, что при наличии уже построенной «правильной» модели угроз и привязки актуальных угроз к мерам из «старого» 58 приказа набор доработок/переработок под новые требования может оказаться минимальным, со ссылкой на п. 3[13] и п. 10[14] Приказа № 21 ФСТЭК России. Ведь если актуальные угрозы уже нейтрализованы, в том числе с учетом иных компенсирующих мер, что еще остается сделать?! Только Акт классификации переписать под УЗ.

Существующий набор документов уже достаточен для построения системы защиты. Его уже можно использовать, в том числе и не по прямому назначению. Приведем примерный перечень возможных вариантов.

1. Построение системы защиты ПДн в соответствии с требованиями законодательства.

2. Минимизация затрат – организация «бумажной защиты» с формальным выполнением требований, в том числе признание ВСЕХ/многих угроз неактуальными. Особенно эффективно для ИСПДн, обрабатывающих «общедоступные данные», а это УЗ-4 и, соответственно, 27 мер.

3. Обеспечение бюджета на ИБ: обоснование перед руководством необходимости затрат на средства защиты с аргументированием возможных убытков (последствий для субъектов), а также со ссылкой на требования законодательства и возможные штрафы и предписания.

4. Развод начальника на деньги – отличается от предыдущего пункта целью получения денег. В данном случае бюджет обосновывается для получения «отката» от поставщиков, а не для защиты информационных ресурсов.

Еще одним интересным и важным документом является 17 приказ ФСТЭК России, устанавливающий требования по защите государственных информационных систем, в том числе обрабатывающих ПДн. Согласно п. 1 и п. 4 указанного приказа он распространяется не только на государственные и муниципальные органы, но и на те организации, которые обрабатывают указанную информацию или даже предоставляют «вычислительные ресурсы (мощности)».

В статье осталось не освещенным еще множество вопросов, в том числе по практике построения «модели угроз» (как жить в отсутствии «отраслевой модели угроз»): порядок актуализации выбранных угроз (именно здесь происходит отсев необходимых к применению требований) или выбор конкретных СЗИ, реинжиниринг конкретной ИСПДн (зачастую минимальные изменения приводят к существенному снижению затрат по защите), а также контроль, перечень документов, и вообще – что делать, когда пришла проверка. В одной публикации отразить все перечисленные выше аспекты невозможно: на курсах по ПДн рассмотрение этого перечня тем занимает до пяти дней «плюс» еще один день посвящен опыту прохождения проверок по защите ПДн.

Учебный центр в 2011 году прошел проверку Роскомнадзора без замечаний. Поэтому, надеюсь, to be continued… ■

[12] *П. 10. Приказа № 21 ФСТЭК России: «При невозможности технической реализации отдельных выбранных мер… могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных».*

[13] *«Меры по обеспечению безопасности ПДн реализуются в рамках СЗПДн, создаваемой в соответствии с Требованиями к защите ПДн при их обработке в ИСПДн, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности ПДн».*

[14] *«…с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных».*